CUPRINS

CUVANT ÎNAINTE 11

ACTUALITATEA ȘI GRADUL DE STUDIERE ACTUAL AL PROBLEMEI ADUSE ÎN DEZBATERE 13

I - ALGORITMI DE CRIPTARE – PIATRA DE TEMELIE A SECURITĂȚII INFORMATICE 17

1. ELEMENTE DE BAZĂ ÎN UNIVERSUL CRIPTOGRAFIC 18

1.1 TERMINOLOGIE 18

1.2 PRINCIPII GENERALE 21

2. ALGORITMI CU CHEIE SECRETĂ 23

2.1 ALGORITMUL DES 23

2.2 ALGORITMUL T- DES 29

2.3 ALGORITMUL AES 30

2.4 METODE DE ATAC ASUPRA ALGORITMILOR CU CHEIE SECRETĂ 37

3. ALGORITMI CU CHEIE PUBLICĂ 42

3.1 ALGORITMUL RSA 42

3.2. ALGORITMUL EL-GAMAL 45

3.3 ALGORITMUL RABIN 48

3.4 ATACURI ASUPRA ALGORITMILOR CU CHEIE PUBLICĂ 50

4. CRIPTOGRAFIE CUANTICĂ 51

5. CONCLUZII PERSONALE PRIVIND UTILIZAREA ŞI IMPLEMENTAREA ALGORITMILOR DE CRIPTARE 55

5.1 ALGORITMI CU CHEIE SECRETĂ SAU ALGORITMI CU CHEIE PUBLICĂ? 55

5.2 PRIVIRE ASUPRA IMPLEMENTĂRILOR ACTUALE PE SCARĂ LARGĂ ALE SISTEMELOR DE CRIPTARE 60

II – METODE ŞI TEHNICI DE REALIZARE A ASIGURĂRII SECURITĂȚII ÎN CADRUL REȚELELOR DE CALCULATOARE 69

6. SECURITATEA REȚELEI DE SISTEME DE CALCUL 70

6.1 NEVOIA DE SECURITATE A REȚELEI....70
6.2 TIPURI DE ATACURI GENERICE ASUPRA REȚELOR DE DATE....71
6.3 TEORII ȘI PRINCIPII ELABORATE PENTRU SECURIZAREA REȚELELOR DE DATE....71
7. MAPAREA SISTEMELOR DE SECURIZARE PE MODELUL STANDARD OSI AL UNEI REȚELE....77
7.1 SECURITATEA LA NIVEL FIZIC....77
7.2 SECURITATEA LA NIVELUL LEGĂTURII DE DATE....77
7.3 SECURITATEA LA NIVEL DE REȚEA....78
7.4 SECURITATEA LA NIVEL DE TRANSPORT....78
7.5 SECURITATEA LA NIVEL DE APLICAȚIE....78
8. PROTOCOALE SPECIFICE PENTRU SECURIZAREA PRIN CRIPTARE A PACHETELOR DE DATE....79
8.1 PROTOCOALE DE PRIMĂ GENERAȚIE – PRECURSOARELE TEHNOLOGIILOR ACTUALE....81
8.2 PROTOCOALE ACTUALE PENTRU SECURIZAREA PACHETELOR DE DATE....96
9. PACHETE DE DATE CRIPTATE PE BAZA TEHNOLOGIEI CUANTICE....118
9.1 DEZVOLTAREA CRIPTOGRAFIEI CUANTICE ÎN EUROPA....118
9.2 CERCETĂRI PRIVIND CRIPTOGRAFIA CUANTICĂ ÎN ROMANIA....121
10. CONCLUZII PERSONALE PRIVIND PREZENTUL ȘI VIITORUL "PACHETULUI" DE DATE....124
III - INTEGRAREA UNEI SOLUȚII DE CRIPTARE PERSONALE....126
11. PRIVIRE DE ANSAMBLU ASUPRA SUBIECTULUI ASIGURĂRII SECURITĂȚII....127
11.1 EXEMPLE DE ATACURI REALIZATE IN MEDIUL IT....129
11.2 SOLUȚIE PERSONALĂ DE ÎMBUNĂTĂȚIRE A SECURITĂȚII ANTI - PHISHING....131
11.3 SECURIZAREA UNUI ECHIPAMENT INDIVIDUAL UTILIZAT PENTRU CONECTAREA LA O REȚEA DE CALCULATOARE....138
12. METODE DE SECURIZARE FOLOSITE PE SCARĂ LARGĂ....146
12.1 ISTORICUL CRIPTOGRAFIEI ȘI DIVERSE TEHNICI DE CRIPTARE....146
12.2 SOLUȚII DE SECURITATE IMPLEMENTATE PE SCARĂ LARGĂ....154

12.3 ATACURI GENERICE ASUPRA SOLUȚIILOR DE CRIPTARE UTILIZATE PE SCARA LARGĂ 163

13. CONTRIBUȚII PERSONALE - INTEGRAREA METODELOR DE CRIPTARE IN APLICAȚII SOFTWARE COMERCIALE 168

13.1 PROPUNEREA UNUI NOU ALGORITM PENTRU ASIGURAREA SECURITĂȚII PRIN CRIPTARE LA NIVEL DE BIT – MULTILAYERED STRUCTURAL DATA SECTORS SWITCHING ALGORITHM (MSDSSA) 168

13.2 IMPLEMENTAREA UNEI SOLUȚII DE CRIPTARE SOFTWARE BAZATE PE ALGORITMUL MSDSSA 176

14. CONCLUZII FINALE ȘI DIRECȚII DE DEZVOLTARE VIITOARE A CERCETĂRII ȘI APLICĂRII REZULTATELOR EI ÎN PRACTICĂ 181

BIBLIOGRAFIE 183

LISTĂ DE ABREVIERI 194